U.S. House of Representatives

Committee on Government Reform

Sub-committee on Technology, Information Policy, Intergovernmental Relations and the Census

Statement for the Record

Theft of Electronic Data

Patrick P. O'Carroll, Jr.
Acting Inspector General of the Social Security Administration

September 22, 2004

Good morning, Mr. Chairman, Mr. Clay, and members of the Subcommittee. Let me first thank you for the invitation to be here today for this important hearing to discuss the theft of electronic data. The mission of the Social Security Administration (SSA) Office of the Inspector General (OIG) is to protect Social Security programs and operations from fraud, waste, and abuse. As the Federal agency that implements this country's retirement and social welfare programs, it is paramount that the information SSA collects and stores is secure and reliable. SSA maintains sensitive information from wage and earnings to medical information. Most notable is the Social Security number (SSN), which is used to link data to millions of individuals. Protecting Agency information is vital to SSA programs, and any breach of the confidentiality or integrity of its information would seriously jeopardize the Agency's mission and erode the public's confidence in SSA's programs.

In addition to protecting the theft of information held by SSA, we are also concerned about the integrity of the information SSA receives. While new technologies afford us greater flexibility in performing routine activities, they also present new opportunities for misuse. As government continues to embrace the electronic age and moves closer to paperless processing, we must be certain that appropriate safeguards are in place to verify the authenticity of every transaction. As part of our mission, we work cooperatively with the Agency to ensure that SSA has the proper controls in place to preserve the integrity of its data and business processes.

Today, I would like to discuss:

- Why it is important to prevent the theft of electronic data
- What OIG is doing to help SSA prevent electronic data theft
- SSA's electronic data security efforts
- What remains to be done

Why it is important to prevent the theft of electronic data

The information technology revolution has changed the way government and business operates. Today, the growth in computer interconnectivity brings a heightened risk of disruption or sabotage of critical operations, allowing unscrupulous individuals to read or copy sensitive data, and tamper with critical processes. Those who engage in these activities have more tools than ever before. We need to protect the public by preventing disruptions and ensuring that any disruptions are infrequent, manageable, of minimal duration, and cause the least damage possible.

The threat of electronic data theft and other cyber attacks is growing exponentially in severity, frequency, and financial cost. According to one estimate, cyber attacks last year alone cost the U.S. financial sector nearly $1 billion. These times of heightened national security demand coordinated efforts to protect computer systems from external and internal intrusion. We are pleased that this Subcommittee is rigorously assessing the Federal Government's progress to address weaknesses in the security of its computer systems—particularly the protection of information and data from the threat of cyber attacks, theft and other security breaches.

I am also concerned about the escalating occurrences of identity theft, a major result of electronic data theft and the fastest-growing form of white-collar crime in the United States. A year ago the Federal Trade Commission (FTC) reported that 27.3 million Americans were victims of identity theft between 1998 and 2003—including 9.9 million people in the study's final year. In 2003, losses to businesses and financial institutions totaled nearly $48 billion, and consumer victims reported $5 billion in out-of-pocket expenses. Clearly, this is a problem that must be brought under control.

What OIG is doing to help SSA prevent electronic data theft

Over the years, we have raised concerns in testimony and reports and have called for improved security for *all* databases—both public and private sector—that contain SSNs and other sensitive data, both as a homeland security issue and as an identity theft issue. Today, the SSN is a widely used identifier, which can be used to tie multiple records together about a single individual. While phone numbers, addresses, and even names can change, the SSN is constant throughout an individual's life. Because of this, many institutions, including hospitals and some banks and brokerages, use clients' SSNs as an identity confirmation. Other institutions, notably banks, use SSNs as secret passwords that only the owner should know.

While common use of the SSN as an identifier seems reasonable, it is an invitation for identity theft. For example, if someone knows the name and SSN of another individual, they could use this information to access accounts, transfer funds, or make other changes to an account, which has serious repercussions for the true account holder. When SSNs appear with their owners' names on driver's licenses, mailing labels, and university student ID cards, the owners of these SSNs become potential targets. In fact, we are currently reviewing the use of the SSN on student IDs in a nationwide audit that will examine such policies at approximately 100 schools. Perhaps the most important step we can take in preventing SSN misuse is to limit the SSNs easy availability on public documents, and even in electronic forums such as the Internet.

Our investigations in this area reveal how widespread the misuse of SSNs and other sensitive data from public and private sector databases has become. For example, we recently discovered an offer to sell up to 10,000 SSNs with matching names on the eBay web site. These SSNs were used by the University of North Carolina at Pembroke as identifiers for its staff, current students, and applicants. The suspect successfully stole these SSNs and was ultimately sentenced to 5 months' incarceration.

Our Philadelphia Field Division participated in an investigation that found that a former credit card company employee provided several co-conspirators personal information of legitimate account holders. The co-conspirators then used this information to open and transfer money from fraudulent accounts. The former employee was sentenced to 4 years probation and ordered to pay the bank restitution of over $132,800.

In another case, after a year-long identity theft investigation, our agents arrested a man who had more than 250 credit cards—along with identification documents and fraudulent Social Security cards—for aliases he used in an elaborate scheme he began while working as a credit manager at a local furniture store. When the company was sold and his job was terminated, he took several credit reports with him and used those SSNs to get credit cards, bank loans, homes, vehicles, computers and cash. He was sentenced to 25 months in prison, ordered to pay $383,000 in restitution to numerous credit card companies and banking institutions, and ordered to forfeit a home and a recreational vehicle.

The range of sources from which these SSNs and other critical personal information were stolen is alarming—legitimate web sites, universities, credit card companies, and a furniture store. It is not just SSA that has your number—numerous government agencies, companies and individual operators such as doctors and insurance agents have them as well. In fact, it is quite possible that your number has been given without your knowledge to numerous organizations, businesses and individuals. We cannot put the genie back in the bottle, but we must do more to make those who hold this critical information treat it with the same respect they would give to their own bank account numbers.

SSA employee fraud

Although the vast majority of SSA's over 60,000 employees are trustworthy, dedicated civil servants, it only takes one corrupt employees to compromise the integrity of the Social Security system and undermine the public's confidence in SSA's programs. The illicit demand for SSNs increases the profitability of providing genuine SSNs illegally to fraudulent applicants. Consequently, our investigations have found that a number of SSA employees have succumbed to this temptation. While employee fraud comprises very few allegations, we consider this an investigative priority.

I would like to give you a couple of examples of our successful investigations in this area. One scheme promised immigrants a Social Security card and U.S. citizenship for up to $75,000 per person. The woman who ran the operation staged naturalization ceremonies with a fake Federal judge, fraudulently obtaining genuine Social Security cards through a 15-year SSA employee. The ringleader was sentenced to 121 months in prison, and ordered to pay restitution of $349,065 to her victims. The SSA employee resigned and was sentenced to 2 months of incarceration. Two others received probation.

Another investigation revealed a $4.3 million criminal enterprise that provided Social Security cards and other credentials to undocumented aliens. Working with other agencies, we found that an SSA employee processed and knowingly approved fraudulent applications for over 1,700 Social Security cards for approximately $1,000 each. Illegally issued SSNs put the financial integrity of the Social Security system at risk, inhibit the country's efforts to thwart terrorism, permit the potential defrauding of other Federal and State programs, and compromise the safety of American citizens. The SSA employee involved in this scheme lost his job, was sentenced to 71 months in prison, and was ordered to forfeit $1 million and his residence in Lake Dallas, Texas. Three co-defendants were sentenced to as much as 63 months in prison, and another was given probation and home confinement.

We recently completed an audit of the Agency's policies and practices towards employees who have inappropriately accessed and used SSA's information systems and the sensitive information in the systems. We found that SSA has a process in place to review potential employee systems security violations and has taken steps to limit its exposure to employee misuse of its systems, and we have recommended additional improvements.

Other Federal agencies' use of the SSN

Within the confines of SSA, the SSN is protected with numerous controls. However, once SSNs are used for other purposes, SSA does not have control over, or the ability to protect, these numbers. The security of files containing SSNs maintained by agencies and organizations at every level of Government and the private sector is a serious concern to us.

Our 2003 audit report *"Federal Agencies' Controls Over the Access, Disclosure and Use of SSNs by External Entities,"* requested by the Chairman of the Subcommittee on Social Security, House Ways and Means Committee, examined the way Federal agencies disseminate and control the use of SSNs. After consultation with the President's Council on Integrity and Efficiency (PCIE), we agreed to serve as audit lead for 15 participating OIGs and to prepare the final report.

We found that despite safeguards to prevent improper access, disclosure and use of SSNs by external entities, Federal agencies remained at risk to such activity. Of the 15 agencies reviewed:

- Fourteen agencies lacked adequate controls over contractors' access to and use of SSNs (for example, eight agencies had not performed site inspections to ensure contractors had upheld their obligation to protect the confidentiality and security of SSNs).

- Nine agencies had inadequate controls over access to SSNs maintained in their computer systems (for example, one agency granted systems access to its employees before completing background security checks, while others were not monitoring user access to ensure users were still current employees or contractors).

- Two agencies did not have adequate controls over non-Government and/or non-contractor entities' access to and use of SSNs (for example, one OIG reported its agency had no standard contract language to include Privacy Act safeguards).

- One agency did not make legal and informed SSN disclosures (its OIG identified instances in which the agency did not inform research study participants that providing their SSNs was voluntary).

While Federal agencies' efforts cannot eliminate the potential that unscrupulous individuals may inappropriately acquire and misuse SSNs, we believe each Federal agency has a duty to safeguard the integrity of SSNs by reducing opportunities for external entities to improperly obtain and misuse them. Given the potential risk for individuals to engage in such activity, we believe Federal agencies would benefit by strengthening controls over the access, disclosure and use of SSNs by State and local governments and other external entities. Misused SSNs, stolen or misappropriated birth certificates, and false or fraudulently-obtained driver's licenses are the keys to identity fraud in the United States. With any one of these three documents, you can generally obtain the other two. We investigate thousands of SSN fraud and identity theft cases every year, and we often find criminals have not only stolen or forged SSN information, but stolen or forged driver's licenses as well. We maintain a strong working relationship with the American Association of Motor Vehicle Administrators (AAMVA) and have supported the development, deployment, and monitoring of commercial driver's license and motor carrier safety programs throughout the United States.

SSA's electronic data security efforts

SSA has made significant progress in strengthening SSN integrity, implementing important suggestions our office has made, and working with us to find solutions. In November 2001, the Commissioner of Social Security established an Enumeration Response Team (ERT) comprised of Agency executives, including OIG representatives, to identify steps the Agency could take to improve the enumeration process and to enhance the integrity of the SSN. Since that time, the Commissioner and the ERT have implemented numerous policies and procedures designed to better ensure that only individuals authorized to receive an SSN are able to do so. Earlier Agency initiatives included improving its Comprehensive Integrity Review Process to identify enumeration vulnerabilities.

The Agency has also has taken steps to improve the verification of employee data. For example, SSA assists employers with its Employee Verification Service (EVS) for registered employers. The Agency is also piloting an online Social Security Number Verification Service (SSNVS), which allows employers and third parties to verify employees' names and SSNs via the Internet, using information in SSA's records, for wage reporting purposes. SSNVS also indicates if SSA records show that the employee is deceased.

Employers have two online SSNVS options:

- Key in up to 10 names and SSNs at a time and the results are returned in seconds.
- Submit a file containing up to 250,000 names and SSNs per file and the results are returned the next business day.

SSNVS is beneficial because it:

- Helps employers use correct names and SSNs on wage reports.
- Reduces the number of submission errors.
- Offers an additional method of requesting verification services.
- Reduces the number of telephone calls required for employers to verify names and SSNs.

The importance of SSN integrity notwithstanding, I noted earlier that the Agency must secure *all* of its data. The President's Management Agenda (PMA) noted expanded e-Government as a presidential initiative across the Federal government. As we provide more online information and transactions, SSA must ensure that its systems and data are secure.

Over the past few years, we have conducted a number of reviews in accordance with the Federal Information Security Management Act of 2002 (FISMA). These reviews have shown that while SSA is in general compliance with FISMA, additional steps must be taken to achieve full compliance. These reviews assist agency managers in addressing the challenges of systems security. They also provide the Administration and Congress with useful information regarding agency efforts to secure their information systems, including sensitive data and operations.

Further, our annual Financial Statement Audit tests security controls that SSA has in place to protect its information. These tests range from reviewing configuration settings on the Agency's computers to penetration testing against the Agency's firewalls. In past years, our financial statement audits have identified improvements the Agency needs to implement to ensure the protection of its information. For example, we identified a reportable condition related to weaknesses in areas including access control, security monitoring, suitability and continuity of operations. In response, SSA has worked diligently to resolve the issues that generated the reportable condition. Some of these issues have been resolved. The Agency is working to resolve the remaining open issues.

What remains to be done

SSA must remain vigilant to ensure the integrity of all of its data. OIG works closely with SSA to help meet these demands through detailed audits of Agency efforts and careful investigations of specific attempts to breach security in its systems. With wireless technology already widespread and greater potential for its use on the horizon, SSA and all Federal agencies must make certain that there are proper safeguards in place to prevent unauthorized access where these devices are used. With more applications connecting to the web, it is essential that authentication processes are sound and that SSA knows for certain it is communicating with the right person. SSA must continue to strike a balance between the need to be user-friendly and the demands for increased security.

Together with Congress and SSA, we have made important strides in reducing vulnerabilities, and that effort continues. Since SSA's inception, it has maintained a robust program for protection of the personal data it holds in trust for our citizens. As technology has advanced, SSA has kept pace in developing appropriate safeguards against intrusion.

Still, to strengthen our defenses even further, we believe SSA should work with agencies across Government to improve safeguards for data security. We also believe SSA and lawmakers should examine the feasibility of the following initiatives.

- Limiting the SSN's public availability to the greatest extent practicable, without unduly limiting commerce.

- Prohibiting the sale of SSNs, prohibiting their display on public records, and limiting their use to legitimate transactions.

- Enacting strong enforcement mechanisms and stiffer penalties to further discourage SSN misuse.

Conclusion

We appreciate the invitation to speak with this subcommittee and help inform the very important work you do to protect computer systems, information and data from the threat of cyber attacks, electronic data theft and other security breaches. We will continue our vigilance in addressing these issues and stand ready to do more to enhance the safety and well-being of all Americans. I would be happy to answer any questions you may have.

Thank you.